UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,520	11/17/2003	Lionel Belnet	550-482	6838

23117 7590 05/26/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
FLOURNOY, HORACE L	

ART UNIT	PAPER NUMBER
2189	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/714,520	BELNET ET AL.	
	Examiner	Art Unit	
	Horace L. Flournoy	2189	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication. Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *19 and 20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/19/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This Office action has been issued in response to amendment filed 6 March 2006. Claims 1-18 are pending. Applicant's arguments have been carefully and respectfully considered, but they are not entirely persuasive, as will be discussed in more detail below, even in light of the instant amendments. Accordingly, this action has been made FINAL.

ACKNOWLEDGEMENT OF REFERENCES CITED BY APPLICANT

As required by **M.P.E.P.** 609(c), the applicant's submission of the Information Disclosure Statement dated **04/19/2006** is acknowledged by the examiner. As required by **M.P.E.P.** 609(c), a copy of the PTOL-1449 is attached to the instant office action. The examiner did not initial the section of the IDS labeled "Other Documents". The applicant failed to cite the inventor and the filing date of these related U.S. applications (See M.P.E.P. 609.04 (a)).

Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

REJECTIONS BASED ON PRIOR ART

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by **Gardner et al. (U.S. PG PUB No. 2003/0101322 hereafter referred to as Gardner).**

With respect to independent **claims 1 and 10,**

(Note: the examiner interprets independent claims 1 and 10 in the same way because of identical or patentably indistinct limitations)

"A data processing apparatus **[Gardner discloses in paragraph [0002], "Computer systems include at least one processor and memory." See FIG. 3]** *having a secure domain and a non-secure domain,* **[Gardner discloses in paragraph [0189], "secure and non-secure"]** *in the secure domain devices of the data processing apparatus having access to secure data which is not accessible in the non-secure domain* **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory."]**, *the data*

processing apparatus comprising: a device bus; **[Gardner discloses in FIG. 3, the memory unit (element 20) coupled to the processor (element 32) via a device bus (connection between). With respect to this limitation Gardner also discloses the Intel IA-64 architecture which utilizes device bus(es).]"** *a plurality of devices ~~device~~* **[disclosed, e.g. in paragraph [0031] as well as paragraph [0034]]** *coupled to the device bus, ~~and~~ each operable to issue a memory access request pertaining to either said secure domain or said non-secure domain at least one of the devices being operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain;* **[As per this limitation, it is notoriously well known that the Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) comprises a device bus which is operable to issue a memory access request. Gardner teaches in paragraph [0026], that the memory access request can pertain to either a secure domain or a non-secure domain]** *and a memory coupled to the device bus* **[FIG. 3, element 20]** *and operable to store data required by the devices ~~device~~, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data;* **[paragraph [0189]]** *each ~~the~~ device being operable to issue onto the device bus the memory access request* **[paragraph [0026], "access...memory"]** *when access to an item of data in the memory is required,* **[disclosed, e.g. in paragraph [0031] as well as paragraph [0034]]** *the memory access request issued by the device including a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain, and the domain signal being provided for use in*

determining whether the access defined by the memory access request is allowed to proceed. **[Gardner discloses in paragraph [0189], "...secure user processes are distinguished from non-secure user processes by setting a bit in the "magic number" or ELF (Executable and Linkable Format) header...the information for distinguishing between secure and non-secure user processes is contained in a secure memory page in memory 74." As interpreted by the examiner Gardner teaches a bit or "domain signal" which identifies whether the memory access request pertains to said secure domain or non-secure domain as taught further in paragraph [0031] as well as paragraph [0034]].]**

With respect to **claims 2 and 11**,

"A data processing apparatus as claimed in claim 1, wherein for said at least one of the devices, said ~~the device is operable in a~~ plurality of modes **["user processes"]** *are replicated in said, ~~including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the~~ secure domain and said non-secure domain.* **[Gardner discloses in paragraph [0189], "user processes" (see also execution privilege levels) which can be secure "user processes" or "non-secure" user processes ("secure and non-secure user processes").]**

With respect to **claims 3 and 12**,

"A data processing apparatus as claimed in claim 1, wherein the devices **[disclosed, e.g. in paragraph [0031] as well as paragraph [0034]]** *~~device has~~*

have a predetermined pin for outputting the domain signal onto the device bus." **[Gardner discloses in paragraph [0189], "...secure user processes are distinguished from non-secure user processes by setting a bit in the "magic number" or ELF (Executable and Linkable Format) header...the information for distinguishing between secure and non-secure user processes is contained in a secure memory page in memory 74."]**

With respect to **claims 4 and 13**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein in said non-secure domain said at least one of the devices ~~device~~ is operable under the control of a non-secure operating system,* **[Gardner discloses in paragraph [0004], "...user applications employ a non-privileged instruction set provided by the processor hardware and an application program interface (API) defined by the operating system." Gardner also teaches in paragraph [0188], that in a non-secure domain the device is operable under the control of a non-secure operating system: "...non-secure application (running at PL3), such as an end user application 44."]** *" and in said secure domain said at least one of the devices ~~device~~ is operable under the control of a secure operating system."* **[Gardner discloses in paragraph [0033], "End user applications 44 run at the least privileged level, PL3, as unprivileged tasks under the control of an operating system image 42 in a secure platform 40 protection domain."]**

With respect to **claims 5 and 14**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *further comprising partition checking logic coupled to the device bus* **[SPK of FIG. 3, element 36]** *and operable whenever the memory access request as issued by one of the devices ~~device~~ pertains to said non-secure domain to detect if the memory access request is seeking to access the secure memory, and upon such detection to prevent the access specified by that memory access request."* **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory."] (Also see paragraphs [0195] and [0146]).**

With respect to **claims 6 and 15**,

"A data processing apparatus as claimed in claim 5 **[see rejection of claim 5]**, *wherein the partition checking logic is managed by one of the devices ~~device~~ when operating in a predetermined secure mode in said secure domain."* **[Gardner discloses in paragraph [0195], "Using the memory management services of SPK 36, a user application is able to create secure memory partitions and processes..."]**

With respect to **claims 7 and 16**,

"A data processing apparatus as claimed in claim 5 **[see rejection of claim 5]**, *wherein the partition checking logic is provided within an arbiter coupled to the device bus* **[SPK of FIG. 3, element 36]** *to arbitrate between memory access*

requests **[paragraphs [0133]-[0135]]** *issued on the device bus."* **[stated supra in rejection of claim 1]**

With respect to **claims 8 and 17**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein said at least one of the devices ~~device~~ is a chip incorporating a processor* **[paragraph [0003]]**, *the chip further comprising a memory management unit...***[Gardner discloses in paragraph [0022], "SPK 36 is preferably a small kernel of trusted, provably correct code that performs all security critical services. Example security critical services include memory and process management..."]** **(FIG. 3)** *operable, when the processor generates the memory access request* **[see rejection of claim 1]**, *to perform one or more predetermined access control functions to control issuance of the memory access request onto the device bus."* **[Gardner discloses in paragraphs [0134]-[0135], "SPK 36 provides abstractions to allocate, map, unmap, and free virtual addresses..."]." (See rejection of claim 7)**

With respect to **claims 9 and 18**,

"A data processing apparatus as claimed in claim 8 **[see rejection of claim 8]**, *wherein the chip further comprises: further memory coupled to the processor via a system bus, the further memory operable to store data required by the processor,* **[Gardner discloses in paragraph [0157], "If the number of active protection keys is greater than the available protection key registers 118, SPK 36 employs the protection key registers as a cache." Gardner teaches**

in FIG.3, a processor (element 32), a cache (element 118), and a further memory unit (element 20), which is coupled to the processor via a system bus (FIG.3) and is operable to store data required by the processor.

Furthermore, Gardner discloses in paragraph [0003], "...The Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) type processors..." It is notoriously well known that the Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) comprises a device bus via which each device is connectable to a further memory unit.]"

"...the further memory comprising secure further memory for storing secure data and non-secure further memory for storing non-secure data; is disclosed in **paragraph [0026] as stated supra (also see rejections of claims 1 and 2).**

"...and further partition checking logic coupled to the system bus and operable whenever the memory access request is generated by the processor when operating in a non-secure mode in said non-secure domain to detect if the memory access request is seeking to access either the secure memory or the secure further memory, and upon such detection to prevent the access specified by that memory access request **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory." Gardner next discloses in paragraph [0195], "Using the memory management services of SPK 36, a user application is able to create secure memory partitions and processes to protect information in memory from all other applications and operating systems running on the system, even including**

the operating system under which it is running."]." (Also see rejection of claim 5)

ACKNOWLEDGMENT OF ISSUES RAISED BY THE APPLICANT

Response to Amendment

Applicant's arguments filed **March 6, 2006** have been fully considered but they are not deemed to be persuasive and, as required by **M.P.E.P. 707.07(f)**, a response to these arguments appears below.

ARGUMENTS CONCERNING *NON*-PRIOR ART REJECTIONS

Double Patenting

The examiner acknowledges the applicant's reply to the provisional double patenting rejection on page 8 of the applicant's remarks. After careful review, the examiner finds the applicant's arguments persuasive and respectfully withdraws the double patenting rejection.

ARGUMENTS CONCERNING PRIOR ART REJECTIONS

1ST POINT OF ARGUMENT:

With respect to the arguments on page 9, line 20 of the applicant's remarks, the examiner respectfully disagrees. Paragraph [0189] of Gardner teaches controlling access to data based on domains and associated domain signals included with memory access requests.

[Gardner discloses in paragraph [0189], "...a secure ELF loader is included among the PL0 services provided by SPK 36 for securely loading secure user applications..." Gardner further discloses in paragraph [0193], "In one embodiment, some secure memory is allocated by calling "secure_malloc( )," which is a PL0 service provided by SPK 36 that allocates memory pages that the user can read and write at PL3, but which are protected using a protection key that is unique to the user's process."] Gardner teaches that SPK 36 can allocate memory while using the ELF to distinguish that memory allocation between secure and non-secure.

2ND POINT OF ARGUMENT:

With respect to the argument on page 10, line 3 of the applicant's remarks, the examiner apologizes for any confusion in the previous Office Action. The examiner equates the plurality of operation modes to "user processes" in paragraph [0189]. As interpreted by the examiner, a "mode" within a secure or non-secure domain is a set of processes, programs, etc. that occur within either a secure or non-secure domain or access designation.

3rd POINT OF ARGUMENT:

With respect to the argument on page 10, line 18, the examiner apologizes for any confusion in the previous Office Action. See the 1st POINT OF ARGUMENT supra. Gardner teaches that SPK 36 can allocate memory while using the ELF to distinguish that memory allocation between secure and non-secure.

4th POINT OF ARGUMENT:

With respect to the argument on page 11, line 8, the examiner interprets, "to proceed" e.g. as analogous to allowing a secure memory access request access secure data pending its domain signal. See the 1st POINT OF ARGUMENT supra. Gardner teaches that SPK 36 can allocate memory while using the ELF to distinguish that memory allocation between secure and non-secure.

5th POINT OF ARGUMENT:

With respect to the argument on page 11, line 12, Gardner does, in fact, teach "a plurality of devices coupled to a device bus, each operable to issue a memory access request..." as cited in paragraph [0031] as well as paragraph [0034], "As illustrated in FIG. 2, a system management counsel (SMC) 70 is coupled to SP computer system 20 via connection 72. In one embodiment, SMC 70 includes separate independent

processors, such as standard non-networked personal computers (PCs). Connection 72 can include serial interfaces (e.g., RS-232 and USB), and/or private LAN connections. SMC 70 is primarily employed to authenticate SPK 36 during SP computer system 20 initialization. In addition, SP computer system 20 is configured via SMC 70." The examiner maintains the rejection of these limitations.

CONCLUSION

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Direction of Future Correspondences

Any inquiry concerning this communication or earlier communication from the examiner should be directed to Horace L. Flournoy whose telephone number is (571) 272-2705. The examiner can normally be reached on Monday through Friday 8:00 AM to 5:30 PM (ET).

Important Note

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reginald G. Bragdon can be reached on (571) 272-4204. The fax phone numbers for the organization where this application or proceeding is assigned is (703) 746-7239.

Information regarding the status of an Application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or PUBLIC PAIR. Status information for unpublished applications is available through Private Pair only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Reginald G. Bragdon
REGINALD G. BRAGDON
PRIMARY EXAMINER

Horace L. Flournoy
Patent Examiner
Art unit: 2189

Supervisory Patent Examiner
Technology Center 2100